Maryland Remote Access Policy

Last Updated: 05/17/2017

Contents

1.0 Purpose

Personnel are increasingly using tools to work remotely. Personnel with **remote access** privileges may access confidential information or resources that must be protected and tracked, especially when accessed from a network or client with a less rigorous security posture than the State. These remote accessing systems may be considered untrusted when they are not controlled by the State (e.g., an employee's personally owned laptop) and pose a risk for data loss or unauthorized disclosure.

The Maryland Department of Information Technology (DoIT) is responsible for, and committed to, managing the confidentiality, integrity, and availability of State government information technology (IT) networks, systems, and applications within the scope of its authority. This includes ensuring that remote connections to the DoIT network or any network managed by State of Maryland Executive Agencies from an outside entity does not endanger the security posture of the State.

The Maryland Department of Information Technology will utilize the baseline controls and standards established by NIST SP 800-53R4 and 800-46R1 to develop this policy.

2.0 Document and Review History

This policy supersedes the Maryland Information Security Policy v3.1 (2013) Section 7: Access Control Requirements. This document also supersedes any policy regarding remote access declared prior to the 2017 Cybersecurity Program Policy, such as the DoIT Remote Access Policy v2.0. This document will be reviewed annually and is subject to revision.

Date	Version	Policy Updates	Approved By:
01/31/2017	v1.0	Approval of Draft	Maryland CISO
5/17/2017	v1.1	Initial Publication	Maryland CISO

3.0 Applicability and Audience

This policy is applicable to all agencies supported by, or under the policy authority of, the Maryland Department of Information Technology, including employees, contractors, vendors and agents of such agencies. DoIT will be responsible for ensuring the security of remote access connections in accordance with the requirements in this policy, and for providing those capabilities to the agencies for which it manages IT.

Agencies under the policy authority, but not under direct management of DoIT, must independently comply with the requirements of this policy if remote access capabilities are offered to their employees, contractors, or vendors.

4.0 Policy

Remote access is defined as any access to an agency information system by a user communicating through an external network such as, for example, the Internet. **Virtual Private Network (VPN)** or equivalent technology should be used when remotely accessing information

systems. All remote access connections that utilize a shared infrastructure, such as the Internet, must utilize some form of encryption for authentication of access credentials and transmission of data.

4.1 General

Remote access methodologies used within the State of Maryland Executive Branch systems will follow the general requirements outlined below.

#	Name	Requirement
A	Approved Methods of Remote Access	Agencies must authorize, document, and monitor all remote access capabilities used on their systems. Approved methods of remote access may include: ▪ Direct Application Access — provides direct access to an application, e.g., user logs into an application IP address ▪ Portal — provides access to multiple applications through a single, authenticating interface; this may take several forms: ◆ Web-portal ◆ Virtual Desktop Infrastructure (VDI) ▪ Remote Desktop Control — provides direct access to a system (and its applications) from a remote location ▪ Tunneling (via VPN) — provides a secure communication channel through which information can be transmitted between networks
B	Business Need	Remote access privileges must be given only to those employees with a clear and documented business need for remote access.
C	Storage of Confidential Information	Storage of confidential information on any non-State owned device is prohibited. Confidential information may not be stored on any State owned, portable device, without prior written approval from: ▪ State CISO (if IT is managed by DoIT through the Enterprise) ▪ Agency Deputy CIO (if not managed by DoIT)
D	Privilege of Remote Access	It is the responsibility of employees and contractors with remote access privileges to ensure that they employ the same security measures and practices as when using an on-site connection. A user with remote access privileges must exercise **due diligence** to protect the device used and information accessed during remote access sessions (see *Acceptable Use Policy*)
E	Compliance with All Policies	All remote access users will comply with all DoIT Cybersecurity Policies and may not perform illegal activities or use the access for outside business interests.

4.2 Requirements

Remote access methodologies used within the State of Maryland Executive Branch systems will have, or be configured to have, the functionalities outlined below.

#	Name	Requirement
A	Authorized Methodology	Agencies who wish to implement remote access solutions to the DoIT or Enterprise network must obtain prior, written approval from DoIT through the State CISO or other delegated authority. Agencies under the authority of DoIT, but not under direct management of DoIT must obtain prior, written approval from their respective Agency Deputy CIO.
B	Multifactor Authentication	All remote access methodologies shall use multifactor authentication for added security measures, where feasible.
C	Centralized Authentication	Any method of remote access must use a centrally managed authentication system for administration and user access.
D	Time-out Requirements	Duration of user sessions must be limited: ▪ A user must re-authenticate to the system after 6 hours ▪ A user session must time-out after 15 minutes of inactivity
E	**Split Tunneling** Forbidden	Reconfiguration of a user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
F	Encryption	▪ All remote access connections that utilize a shared infrastructure, such as the Internet, must utilize encryption for transmission of access credentials and data ▪ Remote access connections must use 196-bit or greater encryption to protect data in transit
G	Anti-virus Updates	All hosts that are connected to State internal networks via remote access technologies must have up-to-date antivirus software implemented.
H	Patching Cadence	All hosts that are connected to State internal networks via remote access technologies must have current operating system security patches installed.
I	User Specific Account	Remote access will be allowed only with the use of unique user credentials.
J	Password Protection	Remote access passwords are to be used only by the individual to whom they were assigned and not to be shared.
K	Server Security	Remote access connections must use the most comprehensive cryptographic protocol available whenever possible (such as TLS 1.2 currently) to ensure data is protected while in transit.
L	Logging	All remotely-connected hosts must have logging enabled (to a syslog server) to collect the following: ▪ Events ▪ User Access ▪ Admin Access
M	Endpoint Security	Endpoint protection technology must be utilized to ensure that personal devices used to connect to State internal networks meet the requirements of State owned equipment for remote access.
N	Remote Access Control Lists	Remote access user lists must be reviewed quarterly and users not active within the last 60 days must be deactivated.

5.0 Exemptions

This policy is established for use within the DoIT Enterprise. If an exemption from this policy is required, an agency needs to submit a DoIT Policy Exemption Form and clearly articulate the reason for the exemption. An operational risk assessment will be conducted to identify the risks and the agency's mitigation strategy associated with this exemption. If the agency can accept the risk, an exemption to this policy may be granted.

6.0 Policy Mandate and References

The Cybersecurity Program Policy mandates this policy. Related policies include:

- Acceptable Use Policy
- Account Management Policy
- Wireless Access Policy

7.0 Definitions

Term	Definition
Due Care	Using reasonable care to protect the interests of an organization. Developing a formalized security structure containing a security policy, standards, baselines, guidelines, and procedures that are implemented through an organization's infrastructure.
Due Diligence	Practices that maintain the **due care** effort. The continued investigation and application of security into the existing infrastructure of an organization.
Remote Access	Ability to access non-public State-managed network resources through an internet accessible device.
Split Tunneling	A computer networking concept which allows a mobile user to access dissimilar security domains like a public network (e.g., the Internet) and a local LAN or WAN at the same time, using the same or different network connections.
Virtual Private Network (VPN)	A virtual network, built on top of existing physical networks that provides a secure communications tunnel for data and other information transmitted between networks.

8.0 Enforcement

The Maryland Department of Information Technology is responsible for enforcing policies for Enterprise onboarded agencies. The DoIT Cybersecurity Program identifies the minimum requirements necessary to comply with the information security standards and guidelines provided within Cyber Security Program Policy and its supporting policies. Agencies not directly managed by DoIT must exercise due diligence and due care to comply with the minimum standards identified by the relevant DoIT policies.

If DoIT determines that an agency is not compliant with this policy or any supporting policy, the non-compliant agency will be given a sixty (60) day notice to become compliant or at least provide DoIT a detailed plan to meet compliance within a reasonable time before the issue is reported to the Secretary of Information Technology. After which, the Secretary of Information

Technology, or a designated authority, may extend a non-compliant agency's window of resolution or authorize a DoIT representative to limit or restrict an agency's access to external and internal communications (effectively shutting down connectivity) until such time the agency becomes compliant.

Any attempt to circumvent remote access policy requirements, such as split tunneling or intentionally sharing confidential information by circumventing encryption, will be considered a security violation and subject to investigation and possible disciplinary action, which may include written notice, suspension, termination, and possible criminal and/or civil penalties.